UNITED STATES DEPARTMENT OF HOMELAND SECURITY

STATEMENT OF KATHLEEN KRANINGER
DIRECTOR OF SCREENING COORDINATION

BEFORE THE U.S. HOUSE OF REPRESENTATIVES
COMMITTEE ON HOMELAND SECURITY

NOVEMBER 8, 2007

INTRODUCTION

Thank you, Chairman Thompson, Ranking Member King, and Members of the Committee for the invitation to appear today. I appreciate this Committee's steadfast support of the Department and your many actions to improve our effectiveness.

At the outset, I would like to acknowledge the strong working relationships we share with the Director of National Intelligence (DNI), the Federal Bureau of Investigation (FBI), the Terrorist Screening Center (TSC), and the National Counterterrorism Center (NCTC), as well as many other federal, state, and local partners working around the clock to protect our country and the American people from terrorist attacks.

None of us alone can keep our nation safe from the threat of terrorism. Protecting the United States is a mission we share and one that requires joint planning and execution of our counterterrorism responsibilities; effective information collection, analysis, and exchange; and the development of integrated national capabilities.

One of the most important tools in the fight against terrorism is the U.S. Government's consolidated Terrorist Watchlist. The implementation and use of the Terrorist Watchlist has enhanced the Department of Homeland Security's (DHS's) screening programs. The use of this single tool across all federal, state and local law enforcement agencies has become one of our most valuable resources in our coordinated fight against terrorist activity. DHS works closely with the FBI and the Office of the DNI to review screening opportunities, implement watchlist enhancements and address potential vulnerabilities. As the largest screening agency, DHS has a significant interest in ensuring the effective and appropriate application of the watchlist in screening programs. This is an iterative process of continual review and improvement. As one example, the Screening Community is focused today on aligning biometric watchlist information in a more automated fashion with biographic records to provide even more efficient screening capabilities.

DHS as a Screening Agency

As you know, U.S. screening efforts start well before individuals arrive in the U.S. Most important, we have a number of information sharing activities with our international allies in the War on Terror. The international community has put significant resources into detecting and tracking terrorist travel across the globe.

Our overseas layers of security related to screening of individuals prior to arrival in the United States include: Department of State (DOS) visa application processing, the Immigration and Customs Enforcement (ICE) Visa Security Units that support DOS screening, and the new Immigration Advisory Program (IAP) that involves screening of travelers by U.S. Customs and Border Protection (CBP) at airports of departure. Currently, CBP maintains IAP deployments in Amsterdam, the Netherlands, Warsaw, Poland, London, Tokyo-Narita, and Frankfurt, Germany. IAP began in Saudi Arabia in 2003, and expanded to four locations in three countries in 2005. Since January 2007, Visa Security Units have been deployed to four additional locations, with plans to deploy to one additional location in November 2007. Watchlist information supports all of these front line officers in their mission to keep dangerous people out of the U.S.

Information-based screening represents the next and most intensive opportunity for screening to prevent terrorists and terrorist weapons from entering the U.S. Leveraging passenger information from both Advance Passenger Information and Passenger Name Record (PNR) data in advance of arrival allows us to check the terrorist watchlist, criminal wants and warrants, and travel history as well as search for connections between known and unknown terrorists. This year we also reached an important agreement with the European Union that will allow us to continue accessing PNR data while protecting passenger privacy.

While we are conducting these checks prior to arrival, DHS is moving toward its Advance Passenger Information System (APIS) pre-departure requirement to perform watchlist checks in advance of boarding. Published in August 2007, the final rule implements the Intelligence Reform and Terrorism Prevention Act of 2004, which requires that electronic manifest information for passengers onboard commercial aircraft arriving in and departing from the United States, and passengers and crew onboard arriving and departing commercial vessels, be vetted by DHS against a government-established and maintained terrorist watch list prior to departure of the aircraft or vessel.

APIS pre-departure is a first step to taking over the No Fly and Selectee list matching responsibility from air carriers. As you know, since 9/11, the U.S. Government has been making the No Fly and Selectee lists available to commercial air carriers flying into, out of, or within the U.S. for passenger prescreening. A nominating agency can recommend that a known or suspected terrorist (KST) be placed on the No Fly or Selectee list if the individual meets specific criteria for inclusion on that list, consistent with the TSC's No Fly and Selectee Lists Implementation Guidance. TSC is ultimately responsible for deciding whether to place individuals on the No Fly or Selectee Lists, which are subsets of Terrorist Screening Data Base.

Today, commercial air carriers are responsible for conducting checks in advance of boarding pass issuance, and they must notify the Transportation Security Administration (TSA) where there is a match to the No Fly list. TSA then notifies the TSC and the FBI, which coordinate the operational response with law enforcement and other agencies and foreign partners as appropriate. Air carriers must also ensure that a match to the Selectee list is subject to secondary screening prior to boarding an aircraft. Note that there are reasons aside from a Selectee match why an individual may be subject to secondary screening including the Computer-Assisted Passenger Prescreening system and random selection.

DHS is preparing to assume responsibility for No Fly and Selectee watch list matching for both international and domestic air passengers through Secure Flight. In August 2007, DHS took a major step forward by publishing the Secure Flight Notice of Proposed Rulemaking. Secure Flight, as outlined in the proposed rule, will make watchlist matching more effective, efficient, and consistent, offering improvements in both security and customer service for the traveling public. DHS expects Secure Flight to add a vital layer of security to our nation's commercial air transportation system while maintaining the privacy of passenger information. Our watchlist matching capabilities will be significantly enhanced when the government takes over this responsibility from air carriers for a number of reasons including the following:

- DHS uniformly will utilize real-time watchlist information;
- Matching will be uniformly conducted by one process with consistent results applied across airlines;
- The system can be effectively and swiftly calibrated to meet the current threat – for example by increasing the number of potential matches that are generated for an intelligence analyst's review, based on an elevated threat;
- Distribution of the watchlists themselves will be more limited – protecting that sensitive information;
- DHS will have passenger information sooner and will be able to adjudicate potential matches prior to the individual's arrival at the airport, thereby reducing the impact of false matches on the traveling public; and
- DHS will have more time to coordinate an appropriate law enforcement response to potential threats and an enhanced capability to stop known or suspected terrorists before they get to the passenger screening checkpoints.

DHS has made substantial progress on Secure Flight, which will establish a more consistent and uniform prescreening process, resulting in enhanced security and reducing potential misidentification issues for legitimate travelers. Despite this progress, the program faces a critical funding shortfall. The current funding level under the Continuing Resolution is significantly lower than the President's total budget request of $74 million ($53 million plus $21 million in a budget amendment submitted this week). In addition, both the House and Senate appropriations marks do not provide adequate funding to move the program to the next phase, operational testing. DHS is working diligently with the Administration and the Congress to address this issue. However, if the current funding level remains, DHS will not be able to operate the program. In mid-December, we will have to suspend essential development contracts and refrain from beginning benchmark and operational testing with airlines. The lack of funding will severely delay rollout of the program and increase costs and risks.

Once inside the U.S., a variety of terrorist-related screening opportunities exist, requiring the discipline in applying risk-based screening measures to ensure that resources are focused accordingly, threats are appropriately addressed and civil liberties and privacy are upheld. DHS screens immigration benefits applicants and critical infrastructure sector workers, consistent with its legal authority through programs such as the Transportation Workers Identification Credential program.

With our current security layers, we have prevented thousands of dangerous people from entering the United States, including individuals suspected of terrorism, murderers, rapists, drug smugglers, and human traffickers. In Fiscal Year 2007, CBP alone encountered 5,953 positive watchlist matches.

I should also dispel some myths about DHS's information-based screening programs. A person's union membership, sexual orientation, and eating habits are irrelevant to DHS's screening programs. All of DHS's information-based screening systems are designed to match travelers against intelligence and/or enforcement information only. Accordingly, DHS only actively seeks data pertinent to screening. However, while screening arriving international passengers via the Automated Targeting System, we may, at times, receive ancillary information from an air carrier or from the individual concerned that could be considered "sensitive." For example, a carrier may note in reservation data that a traveler is blind and will need help finding his seat or that the travel agency that booked the ticket was UnionPlus. From this ancillary information a person could deduce facts about the traveler. However, very pertinent information may also be stored in the same record – including names and passport data. When DHS does receive sensitive data it is because of the need to collect this other relevant information. In these instances, special, stringent protections are put in place to prevent DHS users from viewing any sensitive information unless there is a specific case-related necessity that has been verified by a senior official. DHS is transparent about the rules it has put in place to prevent sensitive information from being used for screening. We have published them in our System of Records Notice for the Automated Targeting System and have made similar public representations to the European Union.

Factors Relevant to Watchlist Matching Effectiveness

Not only is it important to ensure that the watchlist itself is accurate and appropriate to the screening opportunity, but the robustness of the information that is matched against the watchlist is a key factor in effective screening. What level of assurance do we have in the individual's presented identity? What information is provided? As Director Boyle notes in his testimony, different screening opportunities present different challenges. At the border, CBP has many tools at its disposal to identify and screen individuals entering the U.S. – whereas in the current domestic aviation context, we are currently reliant upon the name matching capabilities of the air carriers.

The use of biographic information in screening including reliance on names to identify known of suspected terrorists, has its limitations. For that reason, DHS is pursuing efforts to enhance the effectiveness of the screening conducted at all opportunities by promoting secure identification and the use of biometrics, where appropriate and feasible. US-VISIT biometrics collection that starts overseas during the visa application process provides a significant layer of security. As we move to 10-print collection, our ability to match that information against latent prints from the battlefield or other locations to identify unknown terrorists increases substantially.

Secure identification also enhances our ability to screen effectively. Identification documents often provide the baseline information for conducting screening. For that reason, DHS is pursuing implementation of the Western Hemisphere Travel Initiative (WHTI) and REAL ID.

Both programs are recommendations of the 9/11 Commission, who so aptly noted that "[f]or terrorists, travel documents are as important as weapons." By requiring secure documents to enter the United States, or board commercial aircraft, we will make it harder for people to use fraudulent credentials to travel or cross our borders, and we will make it easier for our CBP Officers to separate real documents from fake, enhancing our security and ultimately speeding up processing.

Misidentification and Redress

Recognizing the impact of screening on the public, particularly where only name-based checks are conducted, agencies have incorporated redress into their screening programs. DHS has implemented the DHS Traveler Redress Inquiry Program (DHS TRIP), which provides a central gateway for travelers to obtain information about screening and redress as well as a central contact to DHS regarding their adverse screening experiences. Travelers, regardless of their nationality, citizenship or residency, can submit inquiries via website, email, or postal mail. The DHS TRIP Program Office then ensures that the cases are reviewed and resolved, to the extent possible, and that travelers receive an official response. The DHS TRIP Program Office, using its redress management system, assigns redress requests to the Department of State or appropriate DHS agencies, ensures coordination of responses, and is instituting performance metrics to track progress, giving leadership visibility into the types of inquiries DHS receives.

Between February 20, 2007, and October 26, 2007, DHS TRIP recorded 15,954 requests for redress in its redress management system and approximately 7,400 cases have been adjudicated and letters have been sent to the travelers. The majority of TRIP requests that remain in process are awaiting submission of supporting documentation by the traveler.

Once a redress request associated with No Fly and Selectee List matching is processed, the cleared individual is also added to the TSA Cleared List that is provided to air carriers. The Cleared List is currently used by the airlines to distinguish false matches from actual matches as they perform No Fly and Selectee List matching.

For international travel, CBP has implemented a process that automatically suppresses specific lookout matches, including terrorist watchlist matches, in its screening systems when a CBP Officer at a port of entry encounters an individual that CBP has previously determined to be a false positive match. When such an encounter is made, the CBP Officer can make a record of this individual's information into the Primary Lookout Override (PLOR) which is an automated system that automatically suppresses that specific hit the next time that person is encountered, unless new derogatory information has become available. As a result, CBP does not have to resolve the false match each time the person travels. From program inception in February 2006 through September 2007, CBP has created 71,487 PLOR records.

Quality Assurance of the Watchlist

In addition to the efforts described above, TSC analysts also conduct various proactive quality assurance projects with support from DHS. We recently completed a review of all records on the No Fly List and are near completion of a record-by-record review of the Selectee List. Quality

assurance projects like the No Fly and Selectee list reviews ensure that the most current, accurate, and thorough watchlist information is made available to DHS and other screening agencies, and that records are updated in a timely fashion. Such regular updates both improve the quality of the screening being conducted and decrease the instances of screening misidentifications.

The U.S. Government is doing much to ensure travelers have the opportunity to seek redress and to enhance the effectiveness of the watchlisting process itself. At the same time, it is worth noting what GAO described in its September 2006 report (GAO-06-1031) – that although the total number of misidentifications is significant, they represent a tiny fraction of the total screening transactions that are conducted on the hundreds of millions of travelers DHS encounters each year.

The DHS Screening Coordination Office, the DHS TRIP Office, and the screening agencies responsible for addressing redress requests continue to refine the concept of operations for DHS TRIP as well as to consider next phases for enhancing the Department's redress capabilities.

Response to GAO Audit

DHS agrees with many of the findings in the GAO Terrorist Watch List Screening report. DHS takes GAO's recommendations seriously and, in fact, has had ongoing efforts to address them.

GAO recommended that the Secretary of Homeland Security "…develop guidelines to govern the use of watchlist records to support private-sector screening processes that have a substantial bearing on homeland security."

In response to this recommendation, DHS is drafting guidelines to establish and support private sector screening for those respective private sector entities that have a substantial bearing on homeland security. These guidelines will prioritize private sector entities by critical infrastructure sector that are necessary for the functioning of our society. For these purposes, critical infrastructure may include, but is not limited to, agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemical industry and hazardous materials, postal and shipping, and national monuments and icons. In addition to the draft guidelines, DHS anticipates preparing an information collection request under the Paperwork Reduction Act, Privacy Impact Assessment, and System of Records Notice, which would address any DHS private sector screening program.

GAO also recommends that the Secretary of Homeland Security "develop and submit to the President through the Assistant to the President for Homeland Security and Counterterrorism an updated strategy for a coordinated and comprehensive approach to terrorist-related screening as called for in HSPD-11" as well as "an updated investment and implementation plan that describes the scope, governance, principles, outcomes, milestones, training objectives, metrics, costs, and schedule of activities necessary for implementing a terrorist-related screening strategy, as called for in HSPD-11." The updated HSPD-11 report is under development and is forthcoming.

The Screening Community has taken extensive steps since 2004 to enhance terrorist screening and many of those efforts that are specific to the watchlist have been outlined in this testimony. Additionally, at the request of the Assistant to the President for Homeland Security and Counterterrorism, DHS is providing such an update to the Homeland Security Council.

CONCLUSION

On September 11, 2001, no one would have predicted the passage of six years without another terrorist attack on U.S. soil. Some believe our country hasn't suffered another attack because we've been lucky. Others contend the terrorist threat has diminished and we are no longer in danger.

I disagree. Over the past six years, we have disrupted terrorist plots within our own country and we have turned away thousands of dangerous people at our borders. We have also witnessed damaging terrorist attacks against some of our staunchest allies in the war on terror.

I believe the reason there have been no additional attacks against our homeland is because we have successfully raised our level of protection and we have succeeded in frustrating the aims of our enemies. That is not to say our efforts have been flawless or that our work is done. On the contrary, we must move forward aggressively to build on our success to keep pace with our enemies.

Our improvements to passenger and cargo screening, critical infrastructure protection, and intelligence fusion and sharing must continue. While no one can guarantee we will not face another terrorist attack in the next six years, if we allow ourselves to step back from this fight, if we allow our progress to halt, if we fail to build the necessary tools to stay ahead of terrorist threats, then we will most certainly suffer the consequences.

I would like to thank this Committee for your ongoing support for our Department. We look forward to working with you and with our federal, state, local, and private sector partners as we continue to keep our nation safe and meet our responsibility to the American people.